A trust-based architecture for managing certificates in vehicular ad hoc networks

Tahani Gazdar, Abderrahim Benslimane, Abderrezak Rachedi, Abdelfettah Belghith

A Trust-based Architecture for Managing Certificates in Vehicular Ad hoc Networks

Tahani Gazdar*‡, Abderrahim Benslimane‡, Abderrezak Rachedi§ and Abdelfettah Belghith*
*University of Manouba, Tunisia
Email: tahani.gazdar@etd.univ-avignon.fr, abdelfattah.belghith@ensi.rnu.tn
‡University of Avignon, France
Email:abderrahim.benslimane@univ-avignon.fr
§University of Paris-Est Marne la Vallée, France
Email: rachedi@univ-mlv.fr

***Abstract*—In this paper, we propose a secure and distributed public key infrastructure for vehicular ad hoc networks VANETs based on an hybrid trust model which is used to determine the trust metric (T_m) of vehicles. The trust model consists on a monitoring system processing on two aspects: the cooperation of vehicles and the legitimacy of the broadcasted data. We propose a fuzzy-based solution in order to decide about the honesty of vehicles. Then, the vehicles which are trusted ($T_m = 1$) and have at least one trusted neighbor can be candidate to serve as certification authorities CAs in their clusters. In order to increase the stability of our distributed architecture, the candidate CA which has the lowest relative mobility will be elected as certification authority CA.**
We conducted a set of simulations in which we evaluate the efficiency and the stability of the clustering algorithm as a function of the speed, the average number of vehicles on the platoon and the percentage of confident vehicles.

I. Introduction

Vehicular networks are characterized by an open architecture that raises tremendous vulnerabilities [1] [2]. Therefore providing information security is a serious challenge in VANETs. In these networks, the significant number of vehicles and the high speed of vehicles bring out important challenges and compel a strong and evolutionary structure for securing communications. Public Key Infrastructure (PKI) is a good promising choice for enabling communications security in vehicular environments. It is based on a trust third parte called certification authority (CA) which is responsible for certifying the public keys of vehicles. However, in MANETs and particularly VANETs, the conception of PKI must take into account the disconnections in the network. Besides, the CA must always be reachable by all vehicles.

In order to circumvent this shortfall, several research works [5], [6], [7] proposed distributing the responsibility of the CA among a set of nodes in the network. Almost proposals use the mobility as metric to elect the vehicles that will assume the role of CA. Unlike these works we propose in this paper a distributed PKI where the CAs are dynamically elected according to not only their mobility but also their trust level since the CA provides a critical service that needs a high level of trustworthiness. We extend our previous work [3] by proposing a new trust model on which is built our architecture of PKI. According to [4] trust management systems target the information itself, they allow the detection of malicious data and dishonest peers. Using our trust model we aim to evaluate the trust level of the vehicles by inspecting the accuracy of the exchanged information. Particularly, we use a fuzzy-based technique in order to filter out fraudulent information and malicious vehicles. The trust metric is updated according to the instantaneous behavior of the vehicles. We consider two aspects of the exhibited behavior: the cooperativeness and the accuracy of the data that the vehicles exchange.

The paper proceeds as follow. In section 2 we discuss the related work. In section 3 we detail our proposal, first we present the trust model, then we describe our distributed PKI. Section 4 depicts the results of simulation. Finally, section 5 concludes the paper.

II. Related Work

In this section, we present some existing works related to the establishment of PKI in VANETs. Additionally, we describe some existing trust models for vehicular networks.

A. Public Key Infrastructure in VANETs

Ramaraj et al. proposed in [5] a self organized key management system based on clusters. In their model, the network is divided into a number of clusters based on the mobility. They admit that in a cluster, vehicles have on average the same velocity, a group can be represented by a single vehicle defined as the cluster head. In their self-organized PKI any user can sign another user's public key. The set of signatures forms the network of trust relationships.
Raya et al. proposed in [6] a distributed PKI for VANET managed by many CAs, each corresponding to a region. The different CAs have to be cross-certified so that vehicles from different regions can authenticate each others. This requires that each vehicle stores the public keys of all CAs whose certificates are needed to be verified.
In [7], authors use a PKI with virtual infrastructure where a set of elected cluster heads are responsible for disseminating messages after digitally signing them. This solution is intended only for the attack called intelligent collisions. However, a PKI in VANETs must cope with different attacks.
Unlike existing architectures and due to the important role

978-1-4673-1950-8/12/$31.00 ©2012 IEEE

of CAs, we admit that only trusted vehicles can assume the responsibilities of CA additionally to the relative mobility metric.

B. Trust Models in VANETs

In VANETs, there exist three types of trust models: 1)Entity oriented, 2)Data oriented and 3)Hybrid models. The entity oriented models require the evaluation of the legitimacy of entities (nodes). In [10], the authors propose a trust model where the vehicles are organized off-line into groups and each group has a reputation value. The group reputation increases if the average of its members'opinion about the road state is conform to the real road state. The limit of this approach is that the reputation of the group is correlated to the behavior of all group members.

The data oriented models require the evaluation of the legitimacy of the information received in the messages. The authors in [11] propose a data-centric trust model. First, each vehicle computes a report about an event by combining static information such as the event type and dynamic information such as the security state of the vehicle. Then all reports about the same event are combined and their validity is inferred by an inference module in order to calculate the posteriori probability of the events. However, since the inference module uses the prior probability, it is not easy to derive it due to the high mobility in vehicular networks.

The hybrid models combine both entity and data oriented approach. In [12], the authors proposed a hybrid approach using a piggybacking technique. Once a vehicle receives a message about an event it appends to the message a trustworthiness opinion about the event before retransmitting it. This opinion is computed combining metrics about direct experiences, indirect trust relationship and opinions of other vehicles received in the message. The drawback of this proposal is that the first opinion attached to the message will affect other opinions since its computing is recursive.

III. The proposed Trust Model

In the proposed architecture, vehicles playing the role of CA are important because they are responsible for certifying vehicles attached to their clusters. To this end, we need trusted parts for issuing certificates.

We propose in this section an hybrid trust model for evaluating the behavior of vehicles and estimating their corresponding trust metric (T_m). The idea consists on the monitoring and the assessment of the behavior of vehicles in two aspects: their cooperativeness in the network and the legitimacy of the information that they broadcast. Each vehicle must monitor all its 1-hop neighbors and calculate their T_m.

In the network, the vehicles broadcast messages related to urgent events occurred on the road which are called *warning messages*. Each time a monitor vehicle receives a warning message, it evaluates the cooperation rate of the source. After, it computes the reputation of the event reported in the received message. Then, using a fuzzy-based approach the monitor filters out malicious vehicles. Finally, according to the outcome of the monitoring process, it updates the T_m of the source. The $T_m(i)$ is a continuous value in [0,1]. The vehicle is trusted (confident) if its T_m reaches 1. In our proposed PKI, only trusted vehicles are allowed to candidate to be CA. Hereafter, we present the different steps followed by a monitor in order to calculate the T_m of its neighbors.

A. Gathering information:

Along its trip, each vehicle broadcasts warning messages that report events happened on the road. In all warning messages, an information about the legitimacy of the event is attached to the messages that we call reputation ($Rep_V(E)$: the reputation of event E computed in vehicle V). In fact, around event E(x,y,t) occurring in position (x,y) and at time t, we consider a static geographic zone Z where vehicles are able to directly detect the event using their on board sensors. The vehicle source of the message affects the reputation value of event E as follow. If vehicle V is in Z and it detects the event, then $Rep_V(E) = 1$, else if vehicle V is in Z and it does not detect E but it receives a warning message about E. Then, it denies event E then $Rep_V(E) = 0$. Otherwise vehicle V calculates an aggregated reputation as described in the following step.

B. Evaluating information:

If vehicle V is beyond Z or it has not an exact information about the reputation of E, it computes $Rep_V(E)$ by aggregating all information about E, which are received from other vehicles in warning messages as follow:

$$Rep_V(E) = \frac{\sum_{i=1}^{i=|S|} Rep_i(E) * d_i * T_m(i)}{\sum_{i=1}^{i=|S|} d_i * T_m(i)} \quad (1)$$

Where S is the set of vehicles from which V receives warning messages about E, $T_m(i)$ is the local trust metric of the vehicle i computed by vehicle V, its default value is $T_m(i) = 0.1$ and d_i is the distance between vehicle i and event E. We use the distance between the vehicle and the event because the closer the reporter is to the event location the more accurate its information on the event will be.

C. Evaluating vehicle behavior

The behavior is evaluated by the monitor, based on the cooperativeness of the monitored vehicle and the legitimacy of the information that it broadcasts, as follow:

- ***The cooperativeness:*** a monitor calculates a forwarding rate called F. It is expressed as the number of messages forwarded by a monitored vehicle divided by the total number of messages transmitted by the monitor vehicle [13]:

$$F = \frac{the\ number\ of\ forwarded\ messages}{the\ total\ number\ of\ transmitted\ messages} \quad (2)$$

- ***The legitimacy of the information:*** Monitor V decides the honesty of monitored vehicle i based on $Rep_i(E)$. We use the fuzzy set theory [9] to classify honesty of vehicles. Each vehicle is classified within one of the

honesty levels. First, an accordance degree corresponding to each vehicle i in S is calculated by monitor V as follow:

$$A_i = \frac{Rep_i(E)}{Rep_V(E)} \quad (3)$$

We define 3 honesty levels represented by fuzzy sets as depicted in figure 1. Then A_i is projected into one of

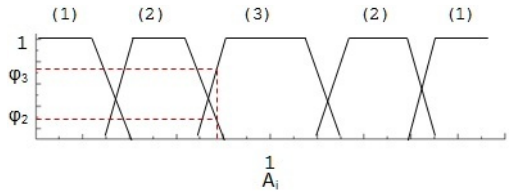


Fig. 1. Membership functions

the trust levels: (1) *malicious* (2) *+/-malicious* or (3) *not malicious*. As expected in figure 1, each fuzzy set F_k has a membership function $\varphi_k : F_k \rightarrow [0, 1]$ determining which honesty level each vehicle is belonging to. Hence, the probability that vehicle V is in honesty level *3 (not malicious)* is computed as follows [8] :

$$P_m = \frac{\varphi_3}{\varphi_1 + \varphi_2 + \varphi_3} \quad (4)$$

D. Updating $T_m(i)$:

Initially the monitor affects $T_m(i) = T_0$ $(0 < T_0 < 1)$ to monitored vehicle i . Then, according to the outcome of the evaluation of the behavior that monitored vehicle i exhibits, the monitor update $T_m(i)$. If P_m is less than threshold δ_2, vehicle i will have $T_m(i) = 0$, and it is declared malicious. Otherwise, if the value of $(F * P_m)$ is greater than threshold δ_1 then $T_m(i)$ increases by γ ($1 \mod \gamma = 0$), otherwise it decreases by γ. If $T_m(i) = 1$, vehicle i is trusted. It is worth mentioning that the values of δ_1, δ_2 and γ are defined as a function of the level of accuracy that we aim to perform towards the evaluation of $T_m(i)$. The detailed algorithm for updating T_m is presented in figure 2.

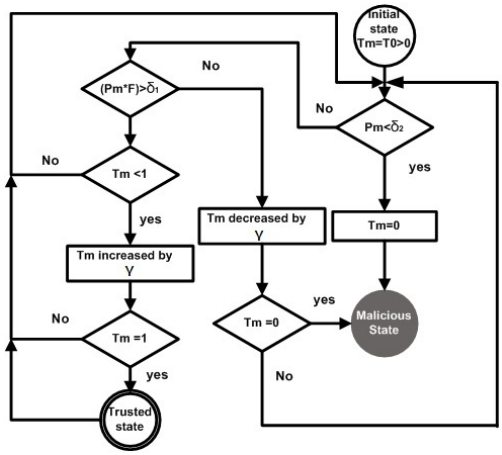


Fig. 2. The State-Transition Diagram of the Trust Model

IV. A DISTRIBUTED PKI FOR VANETS

This section details the clustering phase for electing vehicles which will assume the role of CAs in their clusters.

A. Preliminaries

The basic idea of the proposed architecture consists in establishing a dynamic and distributed public key infrastructure where the role of the CA is distributed among a set of vehicles elected according to a clustering process. The elected clusters heads (CHs) will be the CA in their clusters. A CH is elected according to its trust level T_m, the number of its trusted neighbors and the average of its mobility relatively to its neighbors.

B. Clustering Algorithm

In our clustering algorithm, only trusted vehicles ($T_m = 1$) can be candidate CA. Each vehicle in the network periodically broadcasts a Hello message. It contains information about its current speed, its current position, and T_m of all its neighbors. The Hello messages are broadcasted up to d hops. They are used to build and update the table of neighbors in each vehicle. Particularly, they are used to calculate the average value of T_m for each neighbor. Indeed, upon the receipt of Hello messages, a vehicle updates $T_m(i)$ of each neighbor i as well as its own T_m as follow:

$$T_m(i) = \frac{\sum_{n=1}^{|N|} T_m^n(i)}{|N|} \quad (5)$$

Where: N is the set of Hello messages which contain an information about $T_m(i)$.

Initially, when a vehicle enters in the network it waits during a period of time $timer_1$ for a Hello from an already existing CA or an *election beacon* from a vehicle candidate CA, so that it replies by a *Join* message in order to request for the membership in that cluster. Otherwise, at the expiration of the waiting time, if the vehicle is trusted and if it has at least one trusted neighbor, it can candidate to serve as CA. Indeed, it broadcasts a message called *election beacon* containing its unique identity, the number of its trusted neighbors, its average relative mobility. The *election beacon* is forwarded up to d+1 hops where, d is the maximal size of the clusters dealing with the number of hops between the CH and the farthest vehicle in the same cluster.

Upon the receipt of an *election beacon* a vehicle requests for the membership to the CA originating such *election beacon*. In case where a vehicle receives more than one *election beacon*, its sorts the list of candidates CA according to their relative mobility and the number of their trusted neighbors, in this case the membership request is sent to the header of the list. If the CA accepts the request then it replies with an accept message, otherwise it responds with a reject message. During the clustering process a vehicle passes through a set of states before being attached to a cluster:

- INIT_NODE: a vehicle just entering the road,
- CA_CANDIDATE: a vehicle candidate to be a CA,

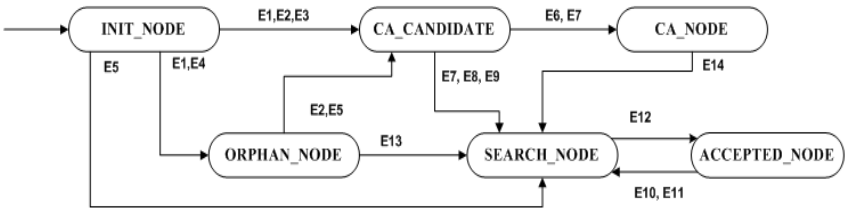


Fig. 3. The state-transition diagram of the clustering algorithm

- ORPHAN_NODE: an orphan vehicle which has no neighbors,
- SEARCH_NODE: a vehicle looking for a CA,
- ACCEPTED_NODE: a vehicle accepted in a cluster.

The clustering algorithm is detailed in the state-transition diagram of figure 3 and the transitions E_i are described in table I. When the CA accepts the membership request of the vehicle, it decides the role of that vehicle in its cluster. In fact, we define 3 types of membership in a cluster:

TABLE I
EVENTS DESCRIPTION

Notation	Event description
E1	$timer_1$ expires.
E2	The vehicle is confident.
E3	The vehicle has at least one confident neighbor.
E4	No HELLO is received.
E5	A HELLO from a confident vehicle is received.
E6	A Join message is received.
E7	$timer_2$ expires.
E8	No Join message is received.
E9	At least a CA candidate exists in neighbors'table.
E10	$timer_3$ expires.
E11	No Accept message is received OR a Reject message is received
E12	An Accept message is received.
E13	A HELLO from a CA vehicle is received.
E14	No RA vehicle still in the cluster.

- RA: Registration Authority. Each trusted vehicle located at 1-hop from the CA acquires the role of RA. The set of RA vehicles constitutes the vehicular dynamic demilitarized zone VDDZ. The role of the VDDZ is to protect the CA from unkown and malicious vehicles.
- GW: GateWay. All vehicles members of at least 2 adjacent clusters acquire the GW state. A GW must have T_m in [0.8,1].
- MN: Member Node. They are simple members of the clusters.

Further details can be found in our previous work [3].

V. PERFORMANCE EVALUATION

In this section we present the results of the simulation. We pointed out the efficiency and the stability of our clustering algorithm.

A. Simulation set up

We conducted a set of preliminary tests using the network simulator OMNET++ [14]. Particularly we used the framework *inetmanet* with the IEEE802.11 MAC layer. We consider a segment of route with a length=10km. The vehicles enter in the network with a rate λ in v/s (vehicles per second). All vehicles have the transmission range equals to 450m. We consider different arrival rate of vehicles as detailed in table II. All clusters have the same maximum size fixed to 300 vehicles. In all simulations, the periodicity of Hello messages is $2s$ and $timer_i = 5s$, i=1,2,3.

TABLE II
THE ARRIVAL RATES

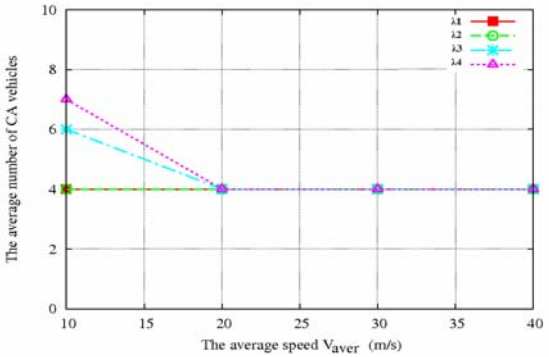
arrival rate (v/s)	Average Speed
λ_1 =0.5	10m/s
λ_2 =1	20 m/s
λ_3 =1.5	30 m/s
λ_4 =2	40 m/s

B. Simulation Results

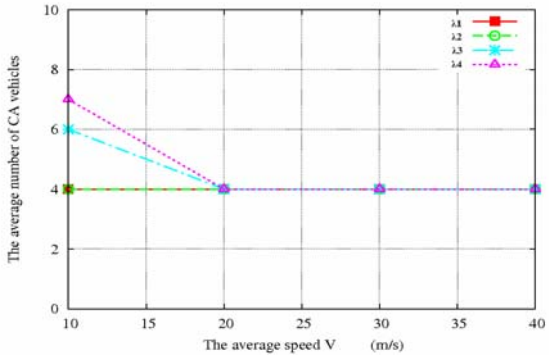
1) The average number of CAs and RAs: We investigate the average number of CAs elected on the platoon and the average number of RA vehicles per cluster. To this end, we plot in figures 4a and 4b the average number of CAs on the road and the average number of RAs per cluster as a function of the average speed and the arrival rate of vehicles for 50% and 100% of trusted vehicles.

At a speed of 10 m/s and $\lambda_4 = 2$v/s, we have on average 2000 vehicles and the maximum range of a cluster is 3. Since the maximum size of a cluster is fixed to 300 vehicles, we need a minimum of 7 cluster heads to cover the entire platoon. With the same speed but for $\lambda_3 = 1.5$v/s, we have instead 1750 vehicles and therefore 6 clusters are enough to cover the entire platoon. For $\lambda_2 = 1$v/s and $\lambda_1 = 0.5$v/s, we have respectively 1000 and 500 vehicles and therefore we require exactly the minimum number of clusters which is 4. From 20 m/s to 40 m/s, the total number of vehicles is less than 1200 for all assumed arrival rates and consequently, only the minimum of 4 clusters is needed to cover the entire platoon. For both cases (50% and 100% of confident vehicles), we found the same result. Indeed, for 100% of confident vehicles we have more confident vehicles which provides more RAs per cluster.

Let us investigate now the average number of RAs per cluster. As depicted in figures 5a and 5b, we clearly observe that the average number of RAs per cluster increases with both the percentage of trusted vehicles and the vehicles arrival rate but decreases when the average speed increases with both

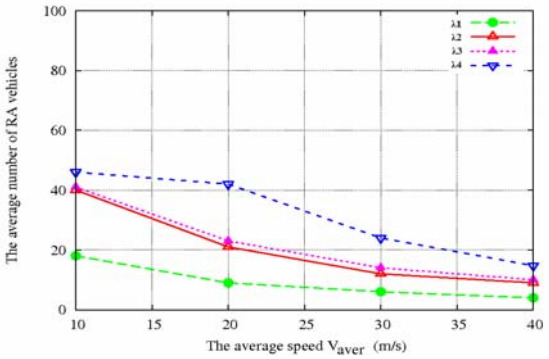


(a) The average number of CAs, 50% of confident vehicles

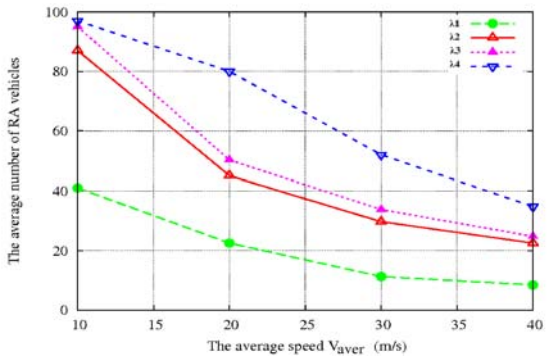


(b) The average number of CAs, 100% of confident vehicles

Fig. 4. The average number of vehicles CA on the platoon



(a) The average number of RAs per cluster, 50% of confident vehicles



(b) The average number of RAs per cluster, 100% of confident vehicles

Fig. 5. The average number of vehicles RA per cluster

the percentage of confident vehicles and the vehicles arrival rate. Indeed, a higher percentage of confident vehicles provides more trusted neighbors to any cluster head and consequently more RAs. This is a positive outcome since a high number of RAs makes more secured the CA.

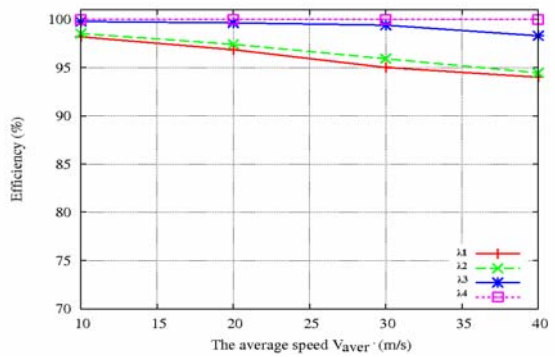
2) Impact of speed and arrival rate on the efficiency: Let us study now the efficiency of the clustering algorithm. The efficiency relies on the percentage of vehicles that acquire a state in a cluster namely CA, RA, MN or GW. We plot in figures 6a and 6b the efficiency as a function of the average speed, the arrival rate of vehicles and two different assumed percentages of confident vehicles. The efficiency stays above 97% for speeds below 20m/s but it lightly decreases for higher speeds. We remark also that it increases as the arrival rate increases. Indeed, for an arrival rate of $\lambda_4 = 2$v/s or even $\lambda_3 = 1.5$ v/s the efficiency stays around 100%. For smaller arrival rates and high speeds, the efficiency decreases. Still yet, the efficiency is rather resilient to the decrease in the percentage of trusted vehicles.

3) Impact of speed and arrival rate on the stability: We investigate the stability of the clustering. Particularly, we are interested in the average life time of CAs. Indeed, the longer the elected CAs can maintain their status, the stronger is the stability of the different memberships. We plot in figures 7a and 7b the average life time of CAs.

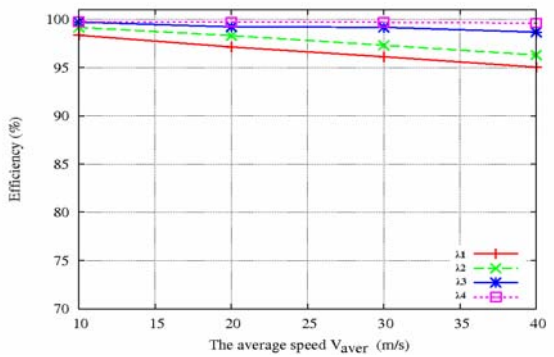
As portrayed in 7b, the life time is about 100%, independently of the speed and the arrival rates of vehicles. This means that any elected CA stays so until it exits from the assumed road segment. Figure 7a shows the same behavior only when the vehicle arrival rate is high (λ_3 and λ_4). However for smaller arrival rates, the average life time of CAs decreases a little bit as the average speed increases. This small decrease is mainly due to the small average number of RAs per cluster at these points. However, the life time stays above 98% even for a speed of 40 m/s. On the other hand and more interestingly we notice that the percentage of trusted vehicles has a small impact on the stability of the clustering scheme.

VI. Conclusion

In this paper, we proposed a distributed and secure architecture for vehicular ad hoc networks. It is based on an hybrid trust model aiming at evaluating the behavior of vehicles.
In our architecture, the responsibilities of CA in the PKI is distributed among a set of vehicles. They are elected according to a clustering algorithm based on two metrics. Only trusted vehicles which have at least one trusted neighbor can candidate to be CA. Besides, in order to enhance the

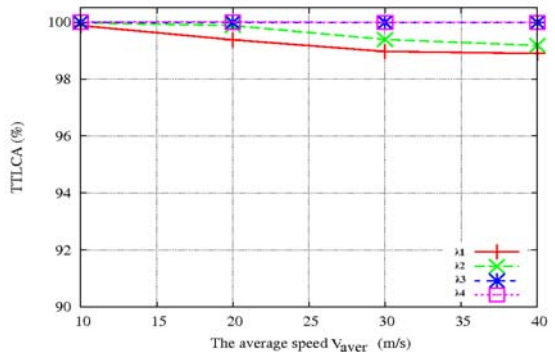


(a) The efficiency of the clustering algorithm, 50% of confident vehicles

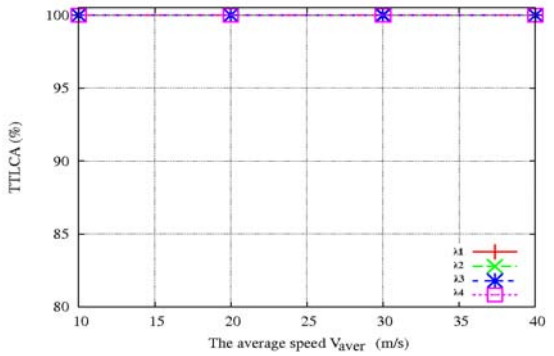


(b) The efficiency of the clustering algorithm, 100% of confident vehicles

Fig. 6. The efficiency of the clustering algorithm



(a) The average life time of CA vehicles, 50% of confident vehicles



(b) The average life time of CA vehicles, 100% of confident vehicles

Fig. 7. The average life time of the CAs

stability of the clustering, the candidate which has the lowest relative mobility will be elected CA. The trustworthiness of vehicles is evaluated throw a monitoring process based on two aspects. First, a monitor evaluates the cooperativeness of monitored vehicles and calculates their forwarding rate. Second, the monitor assesses the legitimacy of information broadcasted by their neighbors. Therefore, according to its trust metric each vehicle acquires a role (i.e :CA, RA, GW or MN) in its cluster. The simulation results out come the efficiency and the stability of the clustering algorithm.
In our future work, we aim to evaluate the performance of our trust model using the simulation.

REFERENCES

[1] P. Papadimitratos, V. Gligor, and JP. Hubaux, *Securing Vehicular Communications - Assumptions, Requirements, and Principles*, in Proceedings of the 4th Workshop on Embedded Security in Cars (ESCAR), November 2006.

[2] B. Parno, A. Perrig, *Challenges in Securing Vehicular Networks*, Proceeding of the Workshop on Hot Topics in Networks (HotNets-IV), 2005.

[3] T. Gazdar, A. Benslimane, A. Belghith, *Secure Clustering Scheme Based Keys Management in VANETs*, The 2011 IEEE 73rd Vehicular Technology Conference (VTC 2011), Budapest, Hungar, May 15-18, 2011.

[4] K. Govindan, P. Mohapatra, *Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey* IEEE Communications Surveys Tutorials Volume PP, Issue 99, pages. 1-20, 2011.

[5] S. Sivagurunathan, P. Subathra, V. Mohan and N. Ramaraj, *Authentic Vehicular Environment Using a Cluster Based Key Management*, European Journal of Scientific Research ISSN Volume 36, Number 2, pages.299-307, 2009.

[6] M. Raya, P. Paradimitratos and JP. Hubaux, *Securing Vehicular Communications*, IEEE Wireless Communications, Volume 13 Number 5 pages. 8-15, October 2006.

[7] J. Blum, A. Eskandarian, *The Threat of Intelligent Collisions*, IT Professional, Volume 6, Number 1, pp.24-29, Jan-Feb 2004.

[8] F. Marmol, G. Perez, *TRIP: a trust and reputation infrastructure-based proposal for vehicular ad hoc networks*, Journal of Network and Computer Applications, March 2011.

[9] F. Marmol, J. Blazquez, G. Perez, *LFTM, linguistic fuzzy trust mechanism for distributed networks*, Concurrency and Computation: Practice and Experience, August 2011.

[10] A. Tajeddine, A. Kayssi, A. Chehab, *A Privacy-Preserving Trust Model for VANETs*, International Conference on Computer and Information Technology, China 2010.

[11] M. Raya, P. Papadimitratos, V. Gligor, J. Hubaux, *On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks*, IEEE Infocom 2008, Phoenix, AZ, USA 2008.

[12] F. Dotzer, L. Fischer, P. Magiera, *VARS: A vehicle Ad hoc network reputation System*, Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, WoWMoM 2005, Taormina-Giardini Naxos 2005.

[13] A. Rachedi, A. Benslimane, *A Secure and Resistant Architecture against Attacks for Mobile Ad Hoc Networks*, Security and Communication Networks, vol.3 NO.2-3 pp. 150-166, 2010.

[14] A. Vargas *OMNeT++ Discrete Event Simulation System User Manual*, March 29, 2005.